UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

_____

Ex parte JUAN A. GARAY and BJORN MARKUS JAKOBSSON

_____

Appeal 2007-0930
Application 10/014,763
Technology Center 2100

_____

Decided: May 18, 2007

_____

Before HUBERT C. LORIN, ROBERT E. NAPPI, and ANTON W. FETTING, *Administrative Patent Judges*.

NAPPI, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 of the Final Rejection of claims 1 through 25. For the reasons stated *infra* we affirm-in-part the Examiner's rejection of these claims.

INVENTION

The invention is directed to a method of generating secure digital signatures with user devices that have limited computational resources (i.e. mobile phone, PDA etc). The user device of limited computational resources generates a first digital signature which can be generated easily; this digital signal is transmitted through an intermediary to a verification unit which after verifying the first digital signature, generates and transmits a second more computationally complex digital signature. See page 3 of Appellants' Specification. Claim 1 is representative of the invention and reproduced below:

1. A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device.

REFERENCES

The references relied upon by the Examiner are:

Micali	US 5,016,274	May 14, 1991
Aura	US 6,711,400 B1	Mar. 23, 2004
		(filed Oct. 14, 1999)

1   REJECTIONS AT ISSUE

2   Claims 2 through 8 stand rejected under 35 U.S.C. § 112 second

3   paragraph as being indefinite. The Examiner's rejection is set forth on pages

4   4 and 5 of the Answer. Claims 1 through 7, 9, 10, 17, and 19 through 25

5   stand rejected under 35 U.S.C. § 102(e) as being anticipated by Aura. The

6   Examiner's rejection is set forth on pages 5 through 9 of the Answer.

7   Claims 8, 11 through 16, and 18 stand rejected under 35 U.S.C. § 103(a) as

8   unpatentable over Aura in view of Micali. The Examiner's rejection is set

9   forth on pages 9 and 10 of the Answer. Throughout the opinion we make

10   reference to the Brief and Reply Brief (filed May 24, 2006, and September

11   11, 2006, respectively), and the Answer (mailed July 13, 2006) for the

12   respective details thereof.

13   ISSUES

14   First issue:

15   Appellants contend that the Examiner's rejection of claims 2 and 3

16   under 35 U.S.C. § 112 second paragraph is in error. Specifically, Appellants

17   argue that the limitations directed to computational efficiency and

18   computational resources are clear. Appellants state:

19   The scope of this limitation would be clear to one skilled in the art in
20   light of the ordinary and customary meanings of the words and their
21   usage in the Specification. Aspects of computational efficiency and
22   computational resources are described in the Specification at, for
23   example, p. 1, lines 12-26 and p. 7, lines 3-8.
24
25   (Same argument presented for claims 2 and 3, Br. 4 and 5)
26
27   The Examiner contends that the rejection is proper. The Examiner

28   states:

As shown above, Examiner would point out that Appellant used
relative terms in the specification for defining/explaining the
computational efficiency. Terms like, "fast", "shorter amount of time",
"less computational complexity" are used in the specification and such
terms are relative terms which need to be some how quantified,
otherwise it would not be clear for one of ordinary skill in the art to
determine with out ambiguity the extent/degree of how
fast/slow/less/short the computational efficiency should be in order to
be compatible with computational resources of the user device. The
office understood the difficulty of quantifying such terms; the point
however is, if such terms are not determined and assigned some
values, one of ordinary skill in the art would not be able to understand
the limitation presented in the dependent claim 2. Therefore the
Rejection under 35 USC § 112 given for dependent claim 2 is proper
and is maintained by the office.

(Same response provided for claims 2 and 3, Answer 11, 12)

Initially, we note that Appellants' arguments on pages 4 through 5 of

the Brief do separately address claims 2 and 3, however, Appellants'

rationale in each argument is the same, thus the issue is dispositive of the

rejection of claims 2 and 3. Appellants' arguments do not address claims 4

through 8 which depend upon claim 3, thus we group claims 4 through 8

with claim 3 see 37 C.F.R. § 41.37(c)(1)(vii).

Thus, Appellants contentions present us with the issue of whether the

claim 2 recitation of "a first digital signature protocol having a

computational efficiency compatible with computational resources of the

user device" and the claim 3 recitation of "second digital signature protocol

having a computational efficiency lower than that of the first digital

signature" clearly delineate the scope of the invention.

1   Second issue:

2   Appellants contend that the Examiner's rejection of claims 1, 2, and

3   19 through 25 under 35 U.S.C. § 102 is improper. Specifically, Appellants

4   assert that the Examiner is improperly equating Aura's authentication center

5   with the claimed user device. Further, Appellants assert that Aura's mobile

6   station does not meet the claimed intermediary device. Appellants state

7   "[t]he intermediary device in claim 1, in contrast, is operative to check that a

8   first signature generated by a user device is valid and to generate a second

9   digital signature which is a returned to the verifier as a signature generated

10 by the user device." (Br. 5).

11 The Examiner contends that the rejection is proper. The Examiner

12 states that Appellants' Specification supports a broad definition of the term

13 "user device" as "any other type of device capable of transmitting or

14 receiving information." Further, the Examiner finds that Aura teaches in

15 figure 4 that the mobile station checks the first signature SRES1 in step 408

16 and generates a second signature SRES2 in step 407.

17 Thus, the contentions of the Appellants present two issues for us,

18 whether the Examiner's interpretation of the claimed "user device" is

19 reasonable and whether substantial evidence supports the Examiner's

20 finding that Aura's user device meets the claimed intermediary device.

21 Third issue:

22 Appellants contend that the Examiner's rejection of claims 8, 11

23 through 16, and 18 under 35 U.S.C. § 103 is improper. Specifically,

24 Appellants assert that the Examiner has not adequately shown that one

25 would be motivated to modify Aura with Micali to arrive at the invention of

26 claims 8, 11 through 16, and 18.

1 The Examiner contends that the rejection is proper. The Examiner's

2 Answer does not provide a direct response to Appellants' contention.

3 Thus, Appellants' contention presents us with the issue of whether the

4 Examiner has established that one would be motivated to combine Aura and

5 Micali to arrive at the claimed invention.

6 FINDINGS OF FACT

7 Facts relating to the first issue:

8 Appellants' Specification discusses portable, "lightweight" devices

9 having limited computational resources. Appellants' Specification further

10 identifies that these limited resources prevent effective implementation of

11 well known digital signature protocols. (Specification 1). Appellants'

12 Specification on page 7 discusses computationally efficient protocols such as

13 Merkle and Lamport signatures which are "fast" and suitable for lightweight

14 devices. (Specification 7). We find Appellants' Specification provides no

15 discussion of metrics used to determine the computational efficiency of a

16 signature protocol, or how it relates to a measure of the resources of the

17 device. Further, Appellants' Specification provides very little insight as to

18 what is considered an effective implementation of a digital signature using a

19 lightweight machine. On page 1 of Appellants' Specification is a discussion

20 of an example of what is apparently a non-effective implementation. In this

21 example Appellants discuss a profile which can take thirty seconds to

22 perform on a portable device such as a telephone.

23 Facts relating to the second issue:

24 Appellants' Specification states on page 5:

25 Although illustrated in this embodiment as a mobile telephone
26 or PDA, the user device 102 may alternatively be implemented as a
27 desktop or portable personal computer, a wearable computer, a

1   television set-top box or any other type of device capable of
2   transmitting or receiving information over network 104. In addition,
3   there may be multiple such devices associated with a given user. For
4   example, a given user may have a mobile telephone as well as a
5   desktop or portable computer, and may utilize both devices for
6   signature generation.
7
8   Aura teaches a method of authentication in a mobile communications

9   system. The system allows for the network to authenticate the subscriber's

10   mobile device and the subscriber's device to authenticate the network. See

11   abstract. In one embodiment the mobile station transmits an international

12   mobile subscriber identity (IMSI) and a random number (RAND1) to a

13   visited public land mobile network (VPLMN). The VPLMN relays this

14   information to the Home listing registry/authentication center (HLE/AUC).

15   See column 6, ll. 21-30. The HLE/AUC retrieves a key Ki from memory

16   (step 403, fig. 4), and generates a second random number (step 404, fig. 4).

17   The HLE/AUC uses the two random numbers, the key, Ki, and three hashing

18   functions to calculate the values SRES1, SRES2' and Kc (step 405, fig. 4).

19   See column 6, ll. 40-45. The values SRES represent a signed response, i.e. a

20   signature. See column 2, l. 60. The values of the second random number

21   RAND2, SRES1, SRES2', and Kc are transmitted to the VPLMN. The

22   VPLMN then transmits the values RAND2 and SRES1 to the subscriber's

23   mobile device. The mobile device also has a key Ki with the same value as

24   the key Ki in the HLE/AUC unit. The Mobile unit uses the values RAND1,

25   RAND2 and Ki to calculate values for SRES1' SRES2 and Kc. See column

26   7, ll. 12-27. The mobile unit compares the received value SRES1 and the

27   calculated value SRES1' (step 408, fig. 4) if they match the mobile unit

28   transmits the value SRES2 to the VPLMN. See column 7, ll. 28 through 34.

1

2   PRINCIPLES OF LAW

3   The purpose of the definiteness requirement is to ensure that the

4   claims delineate the scope of the invention using language that adequately

5   notifies the public of the patentee's right to exclude. *Datamize, LLC v.*

6   *Plumtree Software, Inc,.* 417 F.3d 1342, 1347, 75 USPQ2d 1801, 1804 (Fed.

7   Cir. 2005) (citing: *Honeywell Int'l, Inc. v. Int'l Trade Comm'n,* 341 F.3d

8   1332, 1338 (Fed. Cir. 2003)). Office personnel must rely on Appellants'

9   disclosure to properly determine the meaning of the terms used in the claims.

10 *Markman v. Westview Instruments, Inc.,* 52 F.3d 967, 980, 34 USPQ2d

11 1321, 1330 (Fed. Cir. 1995). "[I]nterpreting what is *meant* by a word *in* a

12 claim 'is not to be confused with adding an extraneous limitation appearing

13 in the specification, which is improper.'" *In re Cruciferous Sprout*

14 *Litigation,* 301 F.3d 1343, 1348, 64 USPQ2d 1202, 1205, (Fed. Cir. 2002)

15 (emphasis in original) (citing *Intervet Am., Inc. v. Kee-Vet Labs., Inc.,* 887

16 F.2d 1050, 1053, 12 USPQ2d 1474, 1476 (Fed. Cir. 1989)). "The scope of

17 claim language cannot depend solely on the unrestrained, subjective opinion

18 of a particular individual purportedly practicing the invention. See

19 Application of Musgrave, 431 F.2d 882, 893 (C.C.P.A. 1970) (noting that

20 "[a] step requiring the exercise of subjective judgment without restriction

21 might be objectionable as rendering a claim indefinite"). Some objective

22 standard must be provided in order to allow the public to determine the

23 scope of the claimed invention." *Datamize v. Plumtree* 417 F.3d at 1350, 75

24 USPQ2d at 1807 (Fed. Cir. 2005). (Emphasis omitted).

25

26

1

2   ANALYSIS

3   Analysis relating to the first issue:

4   Claim 2 recites "a first digital signature protocol having a

5   computational efficiency compatible with computational resources of the

6   user device." As discussed *supra*, we do not find that Appellants'

7   Specification provides a metric for computational efficiency. Appellants'

8   Specification alludes to this being a measure of time that is taken to perform

9   a calculation. However, Appellants' Specification does not provide an

10   objective standard by which it can be determined whether a computational

11   efficiency is compatible with the resources of a device. As such,

12   Appellants' Specification provides no insight as to the actual metes and

13   bounds of the claim, but rather relies upon the subjective criteria of whether

14   something is "fast." Thus, we concur with the Examiner's holding that

15   claim 2 is indefinite as it does not delineate the scope of the invention using

16   language that adequately notifies the public of the patentee's rights.

17   Claim 3 recites, "second digital signature protocol having a

18   computational efficiency lower than that of the first digital signature."

19   Claim 3 is dependent upon claim 2, and thus contains the same

20   indefiniteness problem as claim 2. This indefiniteness is further

21   compounded by the claim 3 recitation of the "computational efficiency being

22   lower" as this implies that a value is assigned to computational efficiency.

23   However as discussed above, we find insufficient evidence to show that the

24   public is notified as to how "computational efficiency" is measured, and as

25   such the scope of the claim. Thus, similar to our holding with respect to

1   claim 2, we concur with the Examiner's holding that claims 3 through 8 are

2   indefinite.

3   Analysis relating to the second issue:

4   Claim 1 recites a "system including at least a user device." As stated

5   by the Examiner the Appellants' Specification provides a list of devices

6   which are user devices and define a user device as being capable of

7   transmitting and receiving information over a network. (Specification 5).

8   Thus, we concur with the Examiner's claim interpretation for the term "user

9   device." However, as argued by Appellants in the Reply Brief on page 3, we

10   find that the Specification implies that a user device is operated by a user.

11   We note, that of the listed devices, not all are operated by direct operation of

12   the user. For example, a set top box typically is operated by a user through a

13   remote control.

14   As discussed *supra,* Aura teaches that the mobile device transmits

15   information to the VPLMN, which relays information to the HLR/AUC.

16   The information is transmitted to the HLR/AUC when the user initiates a

17   connection. In response to receiving this transmission, the HLR/AUC

18   operates to generate and calculate several values which are then transmitted.

19   Thus, we find that the HLR/AUC meets the claim limitation of a user device

20   as it receives and transmits information. Further, we find that the HLR/AUC

21   is user controlled in that it operates in response to user action.

22   Claim 1 further recites, "wherein the verifier sends the first digital

23   signature to the intermediary device, and the intermediary device checks that

24   the first digital signature is a valid digital signature for the user device and if

25   the first digital signature is valid generates a second digital signature which

26   is returned to the verifier as a signature generated by the user device." Thus,

1   the scope of the claimed "intermediary device" is that it checks a first digital

2   signature, generates a second digital signature and transmits the second

3   signature if the first digital signature is verified. As discussed above, we

4   find that Aura's HLR/AUC meets the claimed "mobile device." Further, as

5   discussed *supra,* we find that Aura's mobile station receives a first signature

6   SRES1 and verifies the signatures validity, see step 408 in figure 4. Aura's

7   mobile station also generates a second digital signature SRES2 and transmits

8   it if the first digital signature is valid. Accordingly, we find that Aura's

9   mobile station meets the claimed "intermediary device" as it performs the

10 steps recited as being performed on the intermediary device. Thus, we find

11 for the Examiner on the second issue. Appellants have not presented

12 arguments directed to the separate patentability of claims 2, and 19 through

13 25, accordingly we group these claims together with claim 1 and sustain the

14 Examiner's rejection of claims 1, 2, and 19 through 25 of the reasons stated

15 *supra.*

16   Claim 3.

17   On pages 6 and 7 of the Brief, Appellants argue that the rejection of

18 claim 3 is in error for the reasons asserted with respect to claim 1 and

19 because claim 3 recites the use of two keys which is not taught by Aura.

20 This argument has persuaded us of error in the Examiner's rejection of claim

21 3.

22   Claim 3 recites "the second digital signature is generated using a

23 second secret key associated with second digital signature protocol having a

24 computational efficiency lower than that of the first digital signature

25 protocol." As discussed *supra,* this claim contains several ambiguities,

26 however it is clear from this claim that there are two keys which generate

11

1 different digital signatures. While we do find that Aura teaches two keys

2 with the same value, one in the mobile device and one in the HLR/AUC,

3 these keys are used to generate the same digital signatures. Thus, regardless

4 of the ambiguity of claim 3, we do not find that Aura teaches the limitations

5 of claim 3, and we will not sustain the Examiner's rejection of claim 3.

6 Claims 4 and 5 depend upon claim 3 and are also rejected as being

7 anticipated by Aura. We will not sustain the Examiner's rejection of claims

8 4 and 5 as for the reasons discussed with claim 3.

9 Claims 6, 7, 9, and 10.

10 On pages 8 and 9 of the Brief, Appellants argue that the rejection of

11 claim 3 is in error for the reasons asserted with respect to claim 1 and

12 because Aura does not disclose a secret key pair. Appellants' further

13 arguments have not convinced us of error in the Examiner's rejection of

14 claims 6, 7, 9, and 10.

15 Claim 6 recites "wherein the first digital signature comprises a

16 signature $s1$ on a message m, the signature $s1$ being generated using a secret

17 key s' of a key pair (s', p') associated with the user device." Initially, we

18 note that the term s' and p' are designators and import no meaning into the

19 claim other than to differentiate the keys. Further, we note there is no

20 limitation in claim 6 which recites that the keys s' and p' are of different

21 values or produce different results. Further, we note that the claim is

22 broadly written such that it encompasses the situation where a) key s is

23 associated with the user device and is part of a key pair or b) where the key

24 pair is associated with the user device. It is situation a) that Aura teaches.

25 As discussed above in Aura there is a key Ki in the HLR/AUC (the user

26 device) and another key Ki in the mobile station. The key in the HLR/AUC

1 is used to sign the message sent from the HLR/AUC unit to the LPLMN and

2 the mobile station. The key Ki is kept secret in that it is not transmitted over

3 the air but stored in the HLR/AUC and another copy in the mobile unit's

4 subscriber identity module. See Aura (Col. 2, ll. 11-18). Thus we find

5 ample evidence to support the Examiner's rejection of claims 6, 7, 9, and 10.

6 Claim 17.

7 On pages 9 and 10 of the Brief, Appellants argue that the rejection of

8 claim 17 is in error for the reasons asserted with respect to claim 1 and

9 because claim 17 recites the waiting a predetermined delay between

10 checking that the first signature is valid and sending the second signature.

11 This argument has persuaded us of error in the Examiner's rejection of claim

12 3.

13 As discussed *supra,* in Aura the second signature is sent in response to

14 the determination of the validity of the first signature. While there may be

15 some inherent minimal delay in the performance of this step we do not find

16 that it is of a predetermined amount of time. As we do not find that Aura

17 discloses all of the limitations of claim 17, we will not sustain the

18 Examiner's rejection of claim 17.

19 Analysis relating to third issue.

20 The Examiner's rejection of claims 8, 11 through 16, and 18 on page

21 9 of the Answer states:

22 It would have been obvious to one having ordinary skill in the art, at
23 the time the invention was made, to combine the features of
24 verification digitat [sic] signature using the public key as per teaching
25 of Micali in to the method verification as taught by **Aura,** in order to
26 enhances the security and efficiency of known signature schemes.[See
27 Micali Column 1, lines 7-9].
28

13

1   Initially, we note that of the group of claims included in this rejection,

2   only claims 8 and 11 recite a limitations directed to a public key. As

3   discussed *supra*, in Aura's system the keys Ki are kept secret and not

4   transmitted. We do not find that the Examiner's proffered rationale alone

5   provides sufficient evidence to support a finding that one would be

6   motivated to include public keys especially given the secrecy of the keys in

7   Aura. Accordingly, we will not sustain the Examiner's rejection of claims 8

8   and 11 under 35 U.S.C. § 103. Regarding the Examiner's rejection of claims

9   12 through 16, and 18, the Examiner has not identified where in the evidence

10   of record the limitations of these claims are taught or suggested. Thus, we

11   can not find that the Examiner's rejection of these claims is based upon

12   substantial evidence and we will not sustain the Examiner's rejection of

13   claims 12 through 16, and 18.

14   CONCLUSION

15   We find for the Examiner in that we find that claims 2 through 8 are

16   indefinite as being ambiguous and that Aura anticipates claims 1, 2, 6, 7, 9,

17   10, 17, and 19 through 25. We find for Appellants in that we do not find

18   that Aura anticipates claims 3 through 5 or 17, and we do not find that the

19   combination of Aura and Micali make obvious the limitations of claims 8,

20   11 through 16, and 18. The decision of the Examiner is affirmed-in-part.

21

22

23

24

25

26

1   No time period for taking any subsequent action in connection with

2   this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

3   **AFFIRMED-IN-PART**

4

5

6

7

8

9

10

11

12

13

14

15   rwk

16

17

18

19   Ryan, Mason & Lewis, LLP
20   90 Forest Avenue
21   Locust Valley NY 11560